REV ASSOC MED BRAS. 2013;59(3):209-212

Revista da
ASSOCIAÇÃO MÉDICA BRASILEIRA

www.ramb.org.br

Point of view

Digital signature of medical reports: an issue still not resolved☆

Assinatura digital de laudos médicos: um assunto ainda não resolvido

Aldo von Wangenheim[a], *Ricardo Felipe Custódio*[b], *Jean Everson Martina*[b], *Isabela de Back Giuliano*[c], *Rafael Andrade*[d,*]

[a]*Instituto Nacional para Convergência Digital (INCoD), Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil*
[b]*Computer Security Laboratory – LabSec, UFSC, Florianópolis, SC, Brazil*
[c]*Postgraduate Program in Public Health, UFSC, Florianópolis, SC, Brazil*
[d]*Instituto Federal de Santa Catarina (IFSC), Florianópolis, SC, Brazil*

ARTICLE INFO

Article history:
Received 3 December 2012
Accepted 20 December 2012

No medical practice area is being as affected by the massive introduction of telediagnosis as cardiology.[1] In 2011, in the state of Santa Catarina (SC), Brazil, the Santa Catarina State Integrated Telemedicine and Telehealth System (STT/SC),[2] an initiative responsible to the state government for performing telediagnosis activities for the Brazilian Unified Health System (Sistema Único de Saúde - SUS) in SC, was responsible for carrying out 105,025 tele-electrocardiography examinations, which, according to the Outpatient Information System (Sistema de Informações Ambulatoriais -SIA/SUS), represented 29% of the total of electrocardiographic examinations performed by the SUS in SC during this period. In many cities in the countryside of SC, the practice of cardiology telediagnosis enabled an increase in the offer of electrocardiography examinations by over 300%, which certainly will change the morbidity profile of this population over the next five or ten years.[3] The practice of telecardiology has come to stay; satisfaction studies performed in Santa Catarina have demonstrated that the acceptance and use of this method suggest that its use will only increase.[4]

However, there are still open questions regarding electronic remote issuance of reports, especially with respect to the promises of benefits of digital certification in electronic documents, which must be printed with rigorous authentication and integrity, providing them a legal effect.[5]

☆Study conducted at Universidade Federal de Santa Catarina (UFSC), in a partnership with the Santa Catarina Health Department and Bry Tecnologia, Florianópolis, SC, Brazil.

Corresponding author at: Instituto Nacional para Convergência Digital, Computer Department, Universidade Federal de Santa Catarina, Florianópolis, SC, 88040-900, Brazil.
E-mail: andrade@telemedicina.ufsc.br (R. Andrade).

Digital certification is the only technology capable of safely replacing paper documents signed by physicians for equivalent electronic documents. Electronic documents are easier to circulate, copy, and store; additionally, they can provide more detailed information, such as high quality images and data in formats that preserve its dynamic characteristics, as a film or angiography.[6] However, replacing the physical documents for electronic documents is not easy.[7] There are technological, legal, political, interface, and acceptance challenges to be faced.[5]

In order to sign an electronic document, the physician needs a computer and a digital identity issued by one of the certification authorities accredited by the Brazilian Public Key Infrastructure (Infraestrutura de Chaves Públicas Brasileira [ICP-Brasil]), established by Provisional Measure (MP) 2.200, of August 2, 2001.[8] The digital identity is known in the information technology world as a digital certificate. Linked to the digital certificate is an exclusive cryptographic key pair known as the public key and private key. The private key (or signature key) is used to sign electronic documents, and the public key is used to verify the signature.[9]

Nonetheless, in terms of technology, there are practical issues to be addressed so that physicians have access to digital certification and can trustingly sign their electronic documents. One of these issues regards what is established by the sole paragraph of article six of MP 2.200-2, which imposes on the holder of the digital certificate the sole responsibility for generating the pair of cryptographic keys, with total control over the use of the signature key throughout the entire digital certificate life cycle. It is not simple to apply this standard, since the current technology based on smart cards does not provide such guarantees.[10]

ICP-Brasil established, among others, two main types of digital certificates, A1 and A3. The A1 digital certificate, effective for a maximum period of one year, can have its private key stored in the computer memory. A3 is effective for up to five years and its private key should be generated and maintained in a cryptographic hardware.[11] The most famous are the smart card and the USB cryptographic token. A smart card is a hardware device to store cryptographic keys in a card. A token is a smart card with USB interface.

The control of the private key is much safer using these cryptographic devices than using the computer memory for storage. However, the connection of new peripherals to computers creates a major interoperability problem. If the smart card or the cryptographic token is not properly installed in the computer, users may have problems executing signatures with the key in cryptographic hardware,[9] as the key is restricted to the device – if the device is not accessible, the digital signature cannot be performed.

Indeed, the A1 certificate was created for situations where the use of A3 certificates is not possible, such as Web servers and network equipment. The use of A1 certificates is a problem, as it is impossible to impose on the physician the responsibility for using his/her signature key. Conversely, the use of A3 certificates imposes the use of smart cards, which is precisely the solution currently sought by the Federal Medical Council in its digital certification project for physicians.[11]

Is the current solution satisfactory?

The answer is yes and no. Smart cards, as long as they are used in safe environments, such as hospitals intranets, isolated from Internet access, are extremely safe solutions. They may be used with no restrictions, for example, to certify medical prescriptions or reports in controlled environments. However, on a computer with Internet access, as in a physician's office or in a telemedicine system, where the physician may access and sign a document from anywhere, including from a cybercafé in case he/she needs to issue an emergency medical report, the smart card poses a risk. The physician cannot trust the other software that runs in such computers. Thus, a malicious software could even request for a signature of the physician's card without being noticed.[10]

Why does this happen? While the smart card is inserted into the reader connected to a computer, its signature module may be used by any software in that computer. This makes the smart card vulnerable to malicious programs, such as malware, that save the password entered by the user (PIN), capture the communication between the keyboard and the computer (key loggers) and are, then, free to use the smart card. Within seconds people without physical access to the smart card can sign documents on the Internet. It is important to observe that, for the patient, the risk is very small, except in specific cases. But the physician that owns such certificate is the one who may suffer the consequences, according to Brazilian laws and regulations.[8]

Among the problems regarding the massive use of digital signatures in medical environments, interoperability is poorly addressed. The use of smart cards and cryptographic tokens may interpose itself between the medical task and the creation of the electronic document with the digital signature. Problems may arise, for example, upon certifying the electronic report due to problems associated with the installation of the devices. In this case, the physician must be able to conclude the report in another computer provided with interoperability. Undoubtedly, this causes troubles for the physician's activity and takes time that could be used for better purposes.[4]

There are ways to avoid these problems. Having identified this situation, the Computer Safety Laboratory (Laboratório de Segurança em Computação – LabSEC of UFSC), in a partnership with the Brazilian National Institute for Digital Convergence (Instituto Nacional para Convergência Digital – INCoD), the Bry company from SC, and the Santa Catarina State Health Department are performing, for the STT/SC, a research to develop a new form of two-factor authentication digital signature through the FINEP CIM – Saúde project.[12,13]

This project is creating a technology that will allow for safe electronic signature of medical documents anywhere and from any computer. This solution will use storage and use of private keys in signature servers, called hardware security modules (HSMs). HSMs are devices intended to keep cryptographic keys safe that, in addition to resisting to attacks in a more robust way than smart cards, have an integrated audit process to ensure the correct use of the keys. The A3 certificates, to be used by physicians when signing electronic documents, will be used together with unique confirmation passwords generated by the physician's cell phone through an authentication system linked to the HSM.[14]

With this solution, the physician does not need to carry his/her smart card, leaving it connected to a HSM installed in a safe room, an environment built to provide extremely robust physical access control, where high security systems are usually located. The risk of having a password stolen is eliminated by the counter password, which is created and sent to the cell phone and may be used only one time, for example, to validate a batch of documents that a cardiologist issued in a STT/SC session terminated with this counter password. To confirm the electronic signature in a new batch of reports, the physician will have to generate a new counter password in his cell phone that will be valid only for a few minutes, in order to further reduce the risk of invasion.[14]

Therefore, the use of signatures by physicians becomes very simple. All they have to do is request from the system a new signature. The system produces a multidimensional barcode (QRCode) including all information of the document to be signed. Then, the physician uses the camera of his/her cell phone to import all this data. The cell phone screen displays a subscription term for the documents, which explains what this signature is. He/she confirms and enters his PIN in the cell phone. Then, a 6-digit code is generated to validate that signature for the tele-report service and requests the signing of the document to the HSM.[14]

This code generated stores all data of the signing operation; thus, if any malicious agent tries to change any information about the authorization and signature, the HSM, which will effectively sign, denies the request. It is important to highlight that the physician must always validate the information signed in his/her mobile device and, if something is subsequently changed, this will not affect the report stored in the STT/SC server.[14]

In addition to the safety advantages mentioned, the use of such a system enables the physician to effectively issue a report from any computer and at any place, without necessarily having to trust in the computer used. This happens because the whole process of signature confirmation takes place in his/her mobile device and the only thing entered into the unsafe computer is the authorization code linked to that signature. Besides not wasting time with the installation of a token or card in the computer, the physician can be fully sure that the signing process always takes place in the device over which he/she has total control (his/her cell phone).[14]

Another important point about this solution is the case of malicious software installed in the machine where the physician issues the report. Unlike smart cards and tokens, the mobile device solution does not allow for the insertion of a signature without being noticed by the physician. Another major advantage of the proposed system is the maintenance of a history of signatures executed by a physician in his/her cell phone. With this history, in case of reports not signed by the physician, he/she can prove through his/her signature history that the signature is fake.[14]

Does this strategy solve the problems?

It appears so, but the world is always evolving, and a safe solution today may not be safe in the future. As it happens with every security strategy, there will always be people engaged in finding ways of breaking it and, eventually, they will find a way. Here judgement must be used, and the question asked: how hard it is to forge a signature in a piece of paper? Does anyone give a second look to a paper illegibly signed, with a stamp from the Regional Medical Council? In everyday life, the digital signature certainly represents a much safer and more practical solution than paper documents, providing the physician with security and agility. It is important to be constantly questioning and refining technology, to ensure that everyone's legal certainty, including the physician's.

Financial support

This project has received financial support from SES/SC and FINEP, Florianópolis, SC, Brazil.

REFERENCES

1. Andrade R, Wagner HM, Von Wangenheim A. Telemedicina em Santa Catarina, um projeto sustentável. In: XIII Congresso Brasileiro de Informática em Saúde. CBIS; 2012.
2. Andrade R, Macedo DDJ, Wallauer J, Von Wangenheim A. Building a national telemedicine network. IT Professional. 2008;10:12-7.
3. Savaris A, Andrade R, Macedo DDJ, Von Wangenheim A. O uso da telemedicina assistencial assíncrona em larga escala no setor público de saúde. In: CBIS'2008 - XI Congresso Brasileiro de Informática em Saúde. Campos do Jordão, 2008.
4. Von Wangenheim A, Nobre LFS, Tognoli H, Nassar SM, HO K. User satisfaction with asynchronous telemedicine a study of users of Santa Catarina's system of telemedicine and tele health. Telemed J E-Health. 2012;18:339-46.
5. Nobre LFS, Von Wangenheim A, Maia RS, Ferreira L, Marchiori E. Certificação digital de exames em telerradiologia: um alerta necessário. Radiol Bras. 40:415-21.
6. Graham RN, Perriss RW, Scarsbrook AF. DICOM demystified: a review of digital file formats and their use in radiological practice. Clin Radiol. 2005;60:1133-40.
7. Andrade R, Wallauer J, Von Wangenheim A, Macedo DDJ. A telemedicine network using secure techniques and intelligent user access control. In: The 21th IEEE International Symposium on Computer-Based Medical Systems, 2008, Jyväskylä. Proceedings of the The 21th IEEE International Symposium on Computer-Based Medical Systems; 2008.
8. Brasil. Medida provisória nº 2.200-2, 24 agosto 2001. Institui a infraestrutura de chaves públicas brasileira ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília (DF); 2006 [cited 2 Oct 2012]. Available from: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm
9. Stallings W. Cryptography and network security: principles and practice. 5th ed. New Jersey: Prentice Hall Press; 2010.
10. Delaune S, Kremer S, Steel G. Formal analysis of PKCS#11. In: Proceedings of the 2008 21st IEEE Computer Security Foundations Symposium (CSF '08). Washington (DC): IEEE Computer Society; 2008. p. 331-44.
11. Instituto Nacional de Tecnologia da Informação. DOC-ICP-04: requisitos mínimos para as políticas de certificado na ICP-Brasil. V. 5.0 [cited 20 Nov 2012]. Available from: http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/docs13082012/DOC-ICP-04_-_Versao_5.0.pdf

12. Projeto FINEP. Certificado de identificação mobile para acesso seguro a ambientes de telesaúde e telemedicina-CIMSaude [cited 20 Nov 2012]. Available from: http://www.finep.gov.br// fundos_setoriais/ct_saude/resultados/Resultados%20no%20 Portal%20-%20Chamada%20Telessa%C3%BAde%20e%20Telemedicina.pdf
13. Universidade Federal de Santa Catarina. Notícias [cited 20 Nov 2012]. Available from: http://www.inf.ufsc.br/2012/10/30/incod-and-labsec-recebem-visita-do-presidente-do-conselho-federal-de-medicina/
14. Idalino TB, Spagnuelo D. Senhas descartáveis em dispositivos móveis para ambientes de telemedicina. Curitiba: SBSeg; 2012.